Software Safety

Ron Stroup
FAA, Office of Information Services
Process Engineering Division, AIO-200
(202) 493-4390
Ronald.L. Stroup@faa.gov

Acronyms

CRA	Comparative Risk Analysis
FMEA	Failure Modes Effects Analysis
OSA	Operational Safety Assessment
PHA	Preliminary Hazard Assessment
PHL	Preliminary Hazard List
SHA	System Hazard Analysis
SSHA	SubSystem Hazard Analysis

Overview

- Order 8040.4 Safety Risk Management
- Implementation
- Products

Order 8040.4 (1/5)

- Purpose
  - Established safety risk management policy
  - Prescribes procedures for implementing safety risk management and decision-making tool
  - Establishes Safety Risk Management Committee
- Issued by ASY on 6/26/98

Order 8040.4 (2/5)

- Scope
  - Application of a formalized safety risk management process for all high-consequence decisions
    - Result in a statistical increase or decrease in
      - personal injuries
      - loss of life/health
      - change in property value
      - loss.damage to property
      - cost/savings valued at 100,000,000 or more/year

Formalize a common sense approach

Order 8040.4 (3/5)

- Safety Risk Management Policy
  - Plan
    - Risk analysis
    - Risk assessment
    - Prior to commitment of resources
    - Criteria for acceptable risk
  - Hazard Identification
    - List of hazards

Order 8040.4 (4/5)

- Safety Risk Management Policy
  - Analysis
    - Identify both severity and likelihood of occurrence
  - Assessment
    - Impact of risk element to acceptability criteria
  - Decision
    - compare and contrast options

Order 8040.4 (5/5)

- Safety Risk Management Committee
  - Serves as a resource to FAA Organizations
  - Meets periodically to exchange risk management ideas and information
  - Provide advice and counsel to the Office of System Safety (ASY)
- Consists of technical personnel with risk assessment expertise

Implementation

- Safety Risk Management Committee
- Systems Engineering Council
- Systems Safety Working Group
- Changes to FAA Acquisition Management System

Safety Risk Management Committee

- Provides communications and support team to supplement the overall risk analysis capability and efficiency of key FAA organizations
- maintains a risk management resource directory
  - Risk methodologies employed
  - Resource assistance
- Identifying suitable risk analysis tools and training

Systems Engineering Council (1/2)

- Purpose
  - Orchestrates common systems engineering activities across the NAS
  - Responsibility, authority, and accountability for the development, documentation, deployment, control, and monitoring of the systems engineering process.

Systems Engineering Council (2/2)

- Primary functions
  - leadership, Guidance, and vision
  - Development of process
  - Facilitate problem resolution
- Products
  - System Safety Management Plan
  - System Safety Program Plan outline

System Safety Working Group

- Working arm of the Systems Engineering Council
- Assists in supporting and evaluating Operational Safety Assessments

System Safety Working Group

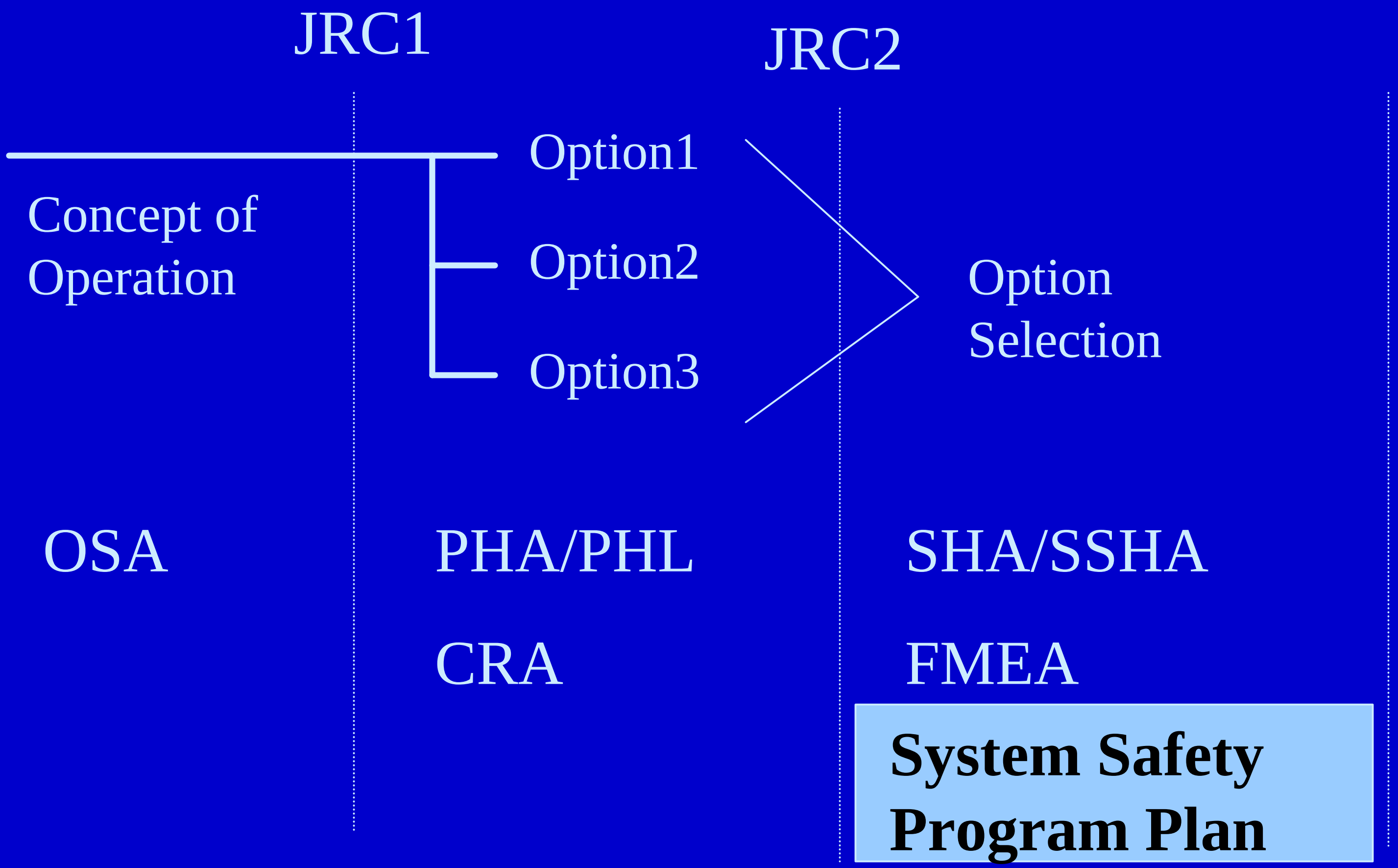
- Products
  - System Safety Handbook
  - System Safety Training
  - SSA Recommendations

Safety process

- Mission Needs
- Investment Analysis
- Solution Implementation
- In-Service Management

SAFETY PLAN

Mission Needs | **Investment Analysis** | **Solution Implementation** | **In-Service Management**



JRC1

JRC2

Concept of Operation

Option1

Option2

Option3

Option Selection

OSA

PHA/PHL

CRA

SHA/SSHA

FMEA

System Safety Program Plan

System Safety Management Plan (Hazard Tracking)

System Safety Handbook

- Outline
- Techniques

System Safety Handbook-Outline

- Ch.1 Introduction
- Ch.2 Policy and Process
- Ch.3 Principles of System Safety
- Ch.4 Pre-Investment Decision
- Ch.5 Post-Investment Decision
- Ch.6 Guidelines for Contracting
- Ch.7 Integrated System Hazard Analysis
- Ch.8 Hazard Analysis Tasks

System Safety Handbook - Outline Contd.

- Ch.9 Analysis Techniques
- Ch.10 System Software Safety
- Ch.11 Test and Evaluation
- Ch.12 Facilities System Safety
- Ch.13 Commercial Launch Safety
- Ch.14 System Safety Training
- Ch.15 Operational Risk Management
- Ch.16 Human Factors

Software Safety Chapter

- Outline
  - What is software safety?
  - Software Safety Planning
  - Safety Critical Software Development
    - Requirements
    - Design
      - Analysis and Design Methods
      - Architecture Design
      - Detailed Design
    - Code
    - Testing

What & Why

- Software safety ensures that the safety risk associated with software performing safety-significant functions is identified, documented, and mitigated.
- It is important because computers have been given the responsibility of autonomous control of safety critical functions and operations.

Software Safety - Planning

- Provisions
  - Consistent definitions of system and software risk
  - Interfaces understood
  - Appropriate verification requirements established
  - Test plans and procedures will achieve verification requirements
- Supports Life Cycle
  - Systems acquisition and systems engineering

Software Safety - Requirements

- Developed
  - Top-down from system requirements
  - Bottom-up from hazards analysis
- Flow-down
  - Checklists and cross-references
  - Requirements criticality analysis
  - Generic Software Safety Requirements

Software Safety - Structured Design

- Techniques
  - Object Oriented Analysis and Design
  - Formal Methods - Specification Development
  - Formal Inspections of specifications
  - Timing, Throughput and Sizing analysis

Software Safety - Architectural Design

- Update Criticality Analysis
- Conduct Hazard Risk Assessment
- Analyze Architectural design
  - Design reviews
  - Simulation
- Interface Analysis
  - Interdependence
  - Independence

Software Safety - Detailed Design

- Design Logic Analysis
- Design Interface Analysis
- Software Fault Tree Analysis

Software Safety - Code

- Code Logic Analysis
- Code Interface Analysis
- Safe subsets of programming languages

Software Safety - Testing

- Test Coverage
- Test Results Analysis
- Independent Verification and Validation

Summary

- Instructions on how to perform system safety engineering and management for FAA personnel involved in system safety activities.

- Emphasis on System Safety Management Plan and System Safety Program Plan